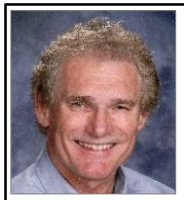
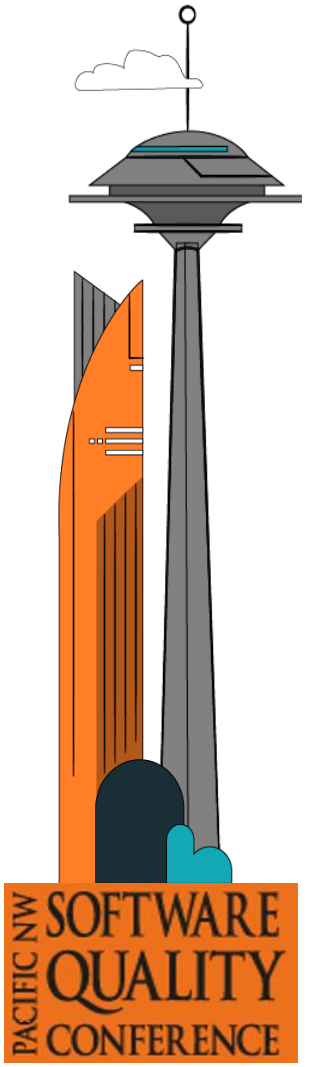
Agent-Based Digital Identity Architecture

Pacific Northwest Software Quality Conference
Portland, Oregon, October 14-16, 2024



Kal Toth

Kalman C. Toth, **Ph.D, P.Eng.**
kalmanctoth@gmail.com
https://www.sovereignimage.com
https://www.linkedin.com/in/kaltoth/



Abstract, Bio, Paper, Presentation Slides

PNSQC 2024 “at-a-glance” and “technical papers”

https://www.pnsqc.org/kal_toth_2024.php

http://www.sovereignimage.com/PNSQC2024/

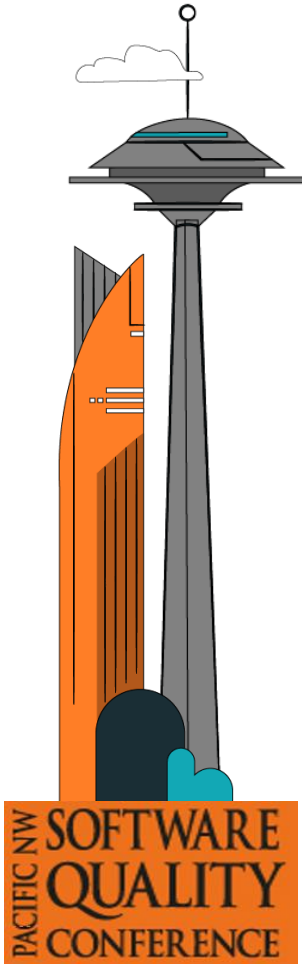
Aspirational Identity Architecture Proposal

- Internet is server-centric
- Missing identity layer and protocols
- Passwords huge inconvenience, unsustainable strategy

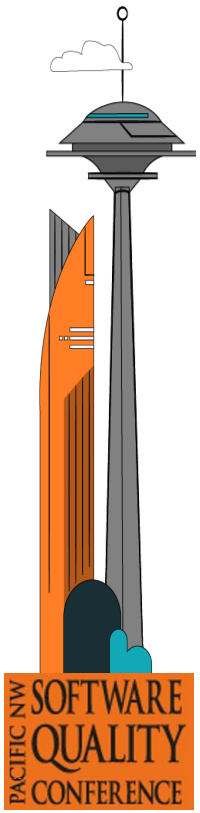
- Countless large-scale breaches
- Ongoing phishing and impersonation attacks
- Wide-spread private data and identifying information abuse

- Kim Cameron (Microsoft): Patchwork of identity schemes
- Tim Berners-Lee: take back power from big players
- Christopher Allen: identity should be “self-sovereign

- W3C: decentralized, machine-readable, verifiable
- Dick Hardt (Sxip): user-centric, rich personas, single protocol



Objective: Decrease Risks by Increasing Solution Strength



breaches, impersonation

data collection, password dependency, complexity, usage

decentralize
self-sovereign
owner-managed
owner-controlled
intuitive, easy-to-use
identity-proofed

identity

solution strength

single sign-on, federated, 2FA, MFA, biometrics

Integrative Digital Identity Solution

A. What One Knows
passwords, PINs

online profiles and passwords managed by users

social networks

professional networks

enterprise solutions

identity access management

federated ID solutions

single sign-on

governmental systems

banking systems

B. What One Holds
devices

WhatsApp

PGP

SMS

Signal

Telegram

loss, theft

C. What One Is biometrics
devices bound to owners

Yubico

Nok Nok

WebAuthn

FIDO

owner-controlled

identity-assured (proofed, attested)

pers. ident. info.

W3C VC model

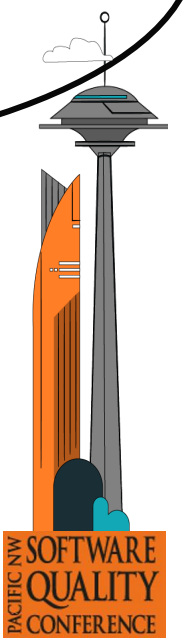
decentralized

W3C DID model

virtualized
intuitive
easy-to-use

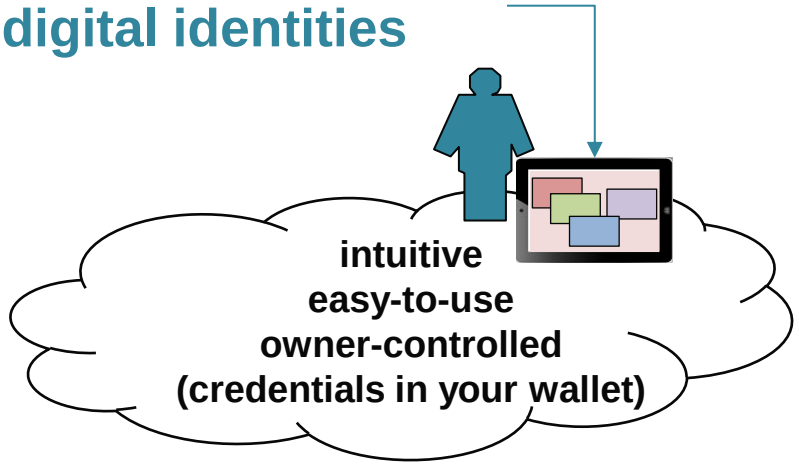
E. What Others Assert
identity-proofed & attested

D. What One Asserts
attributes, images



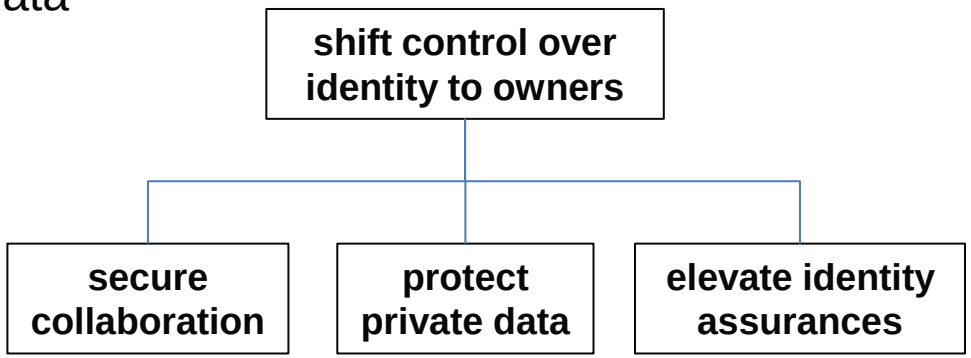
Proposed Features and Capabilities

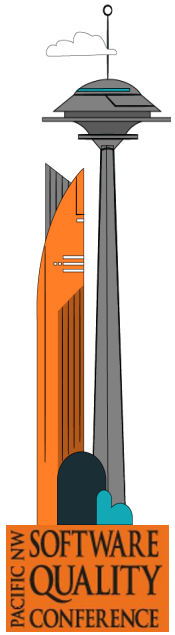
Owners install identity agents on their device(s) for managing digital identities



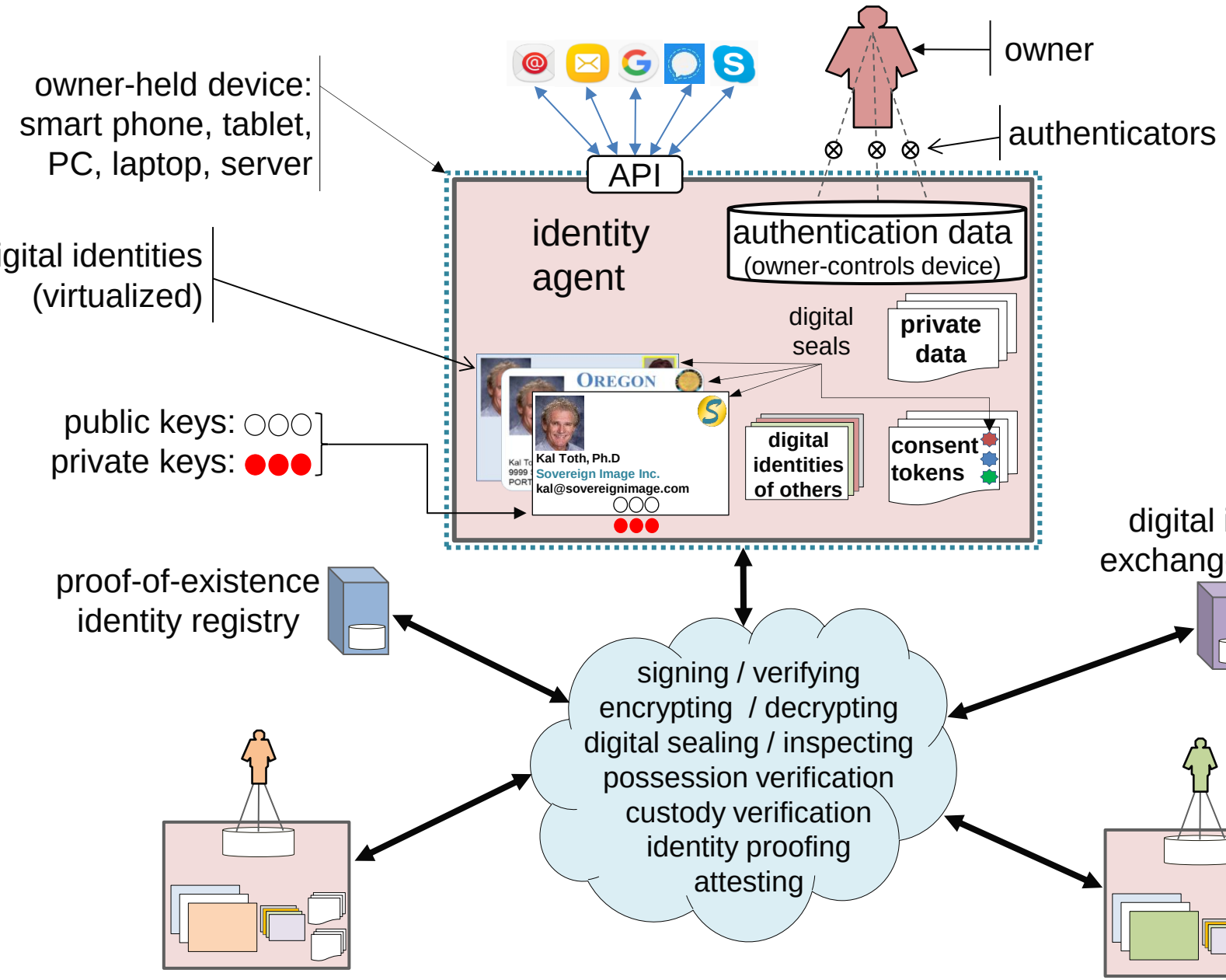
… mimic physical credentials …

- identify and authenticate owners
- sign and encrypt messages, transactions
- encrypt/decrypt private data
- proof, attest, seal digital identities
- use digital identities instead of passwords
- delegate access to private data
- notarize digital documents

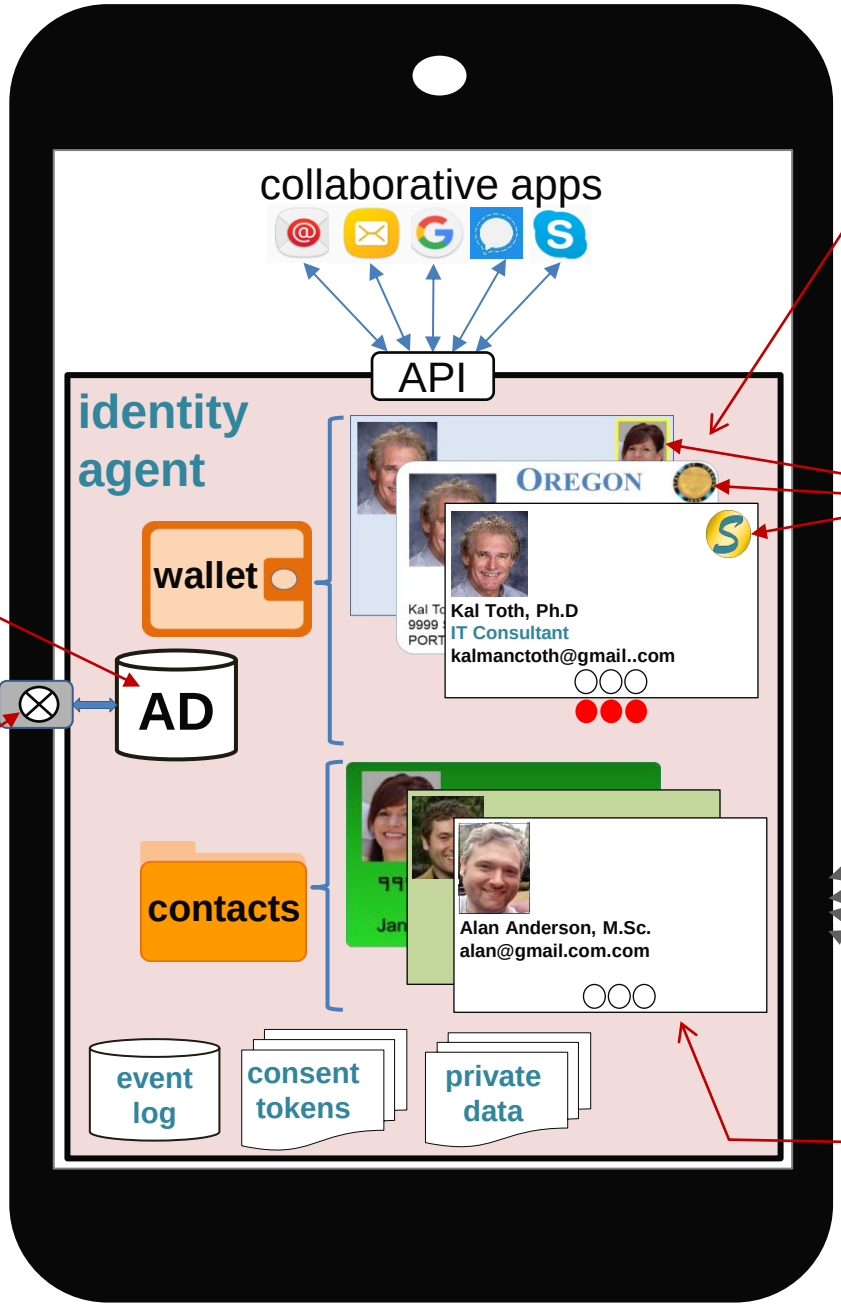




Agent-Based Digital Identity Architecture



Identity Agent Owner's View



digital identities of owner:
(each is a "*sovereign image*")
identifying, anonymous, or pseudonymous; identifier; attributes; sealing image;
private/public key-pairs:
- signing/verifying
- decrypting/encrypting
- embossing/inspecting

affixed digital seals:
- issue date
- attestation
- digital identity identifier
- artifact identifier
- digital seal signature

identifying documents

owner

auth'n data

authenticator (e.g.)
- password / PIN
- fingerprint
- facial recognition
- hand geometry
- iris recognition
- voice recognition

identity agents of other parties

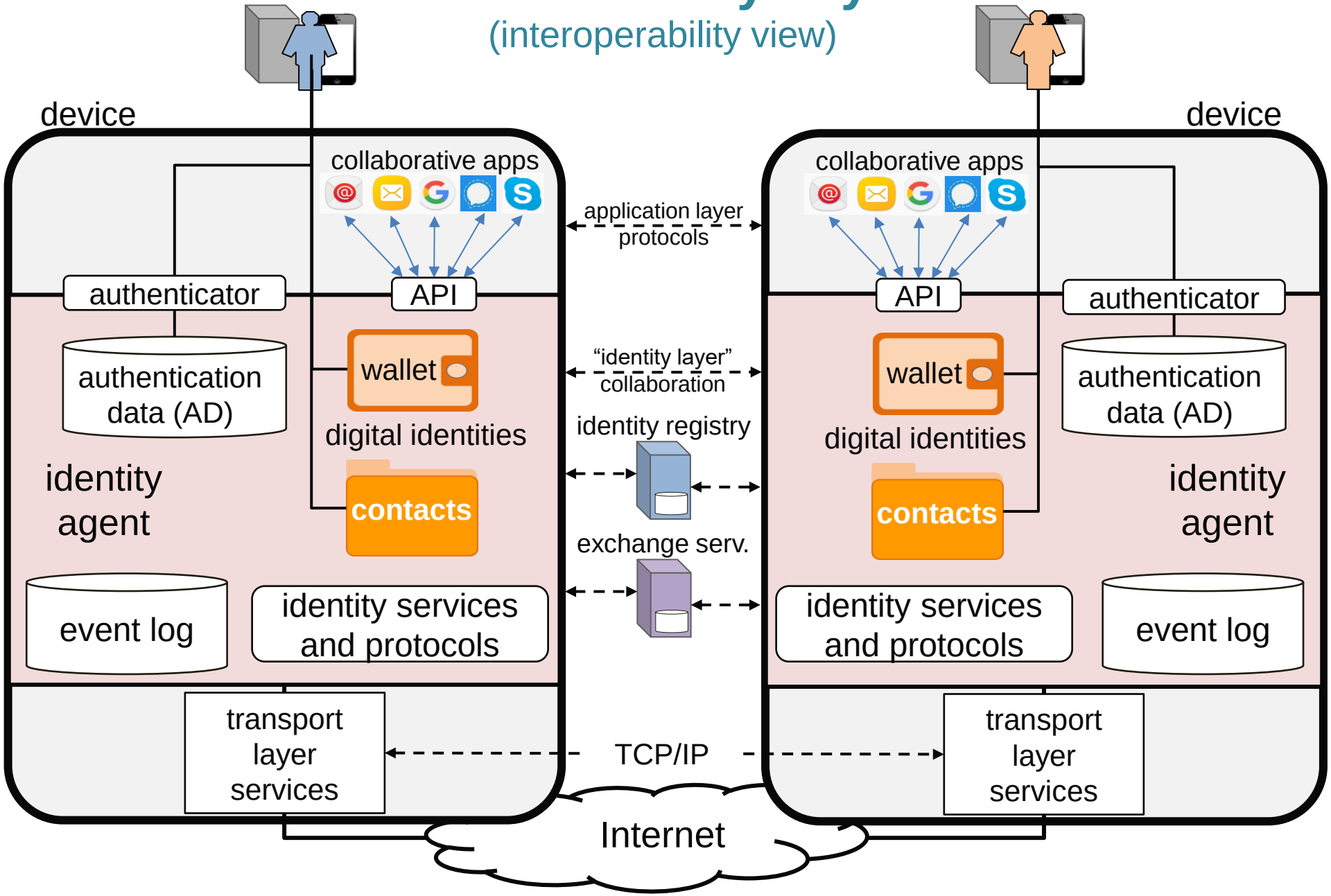
identity registry

exchange service

digital identities of others:
"*public copies*" (public keys only)

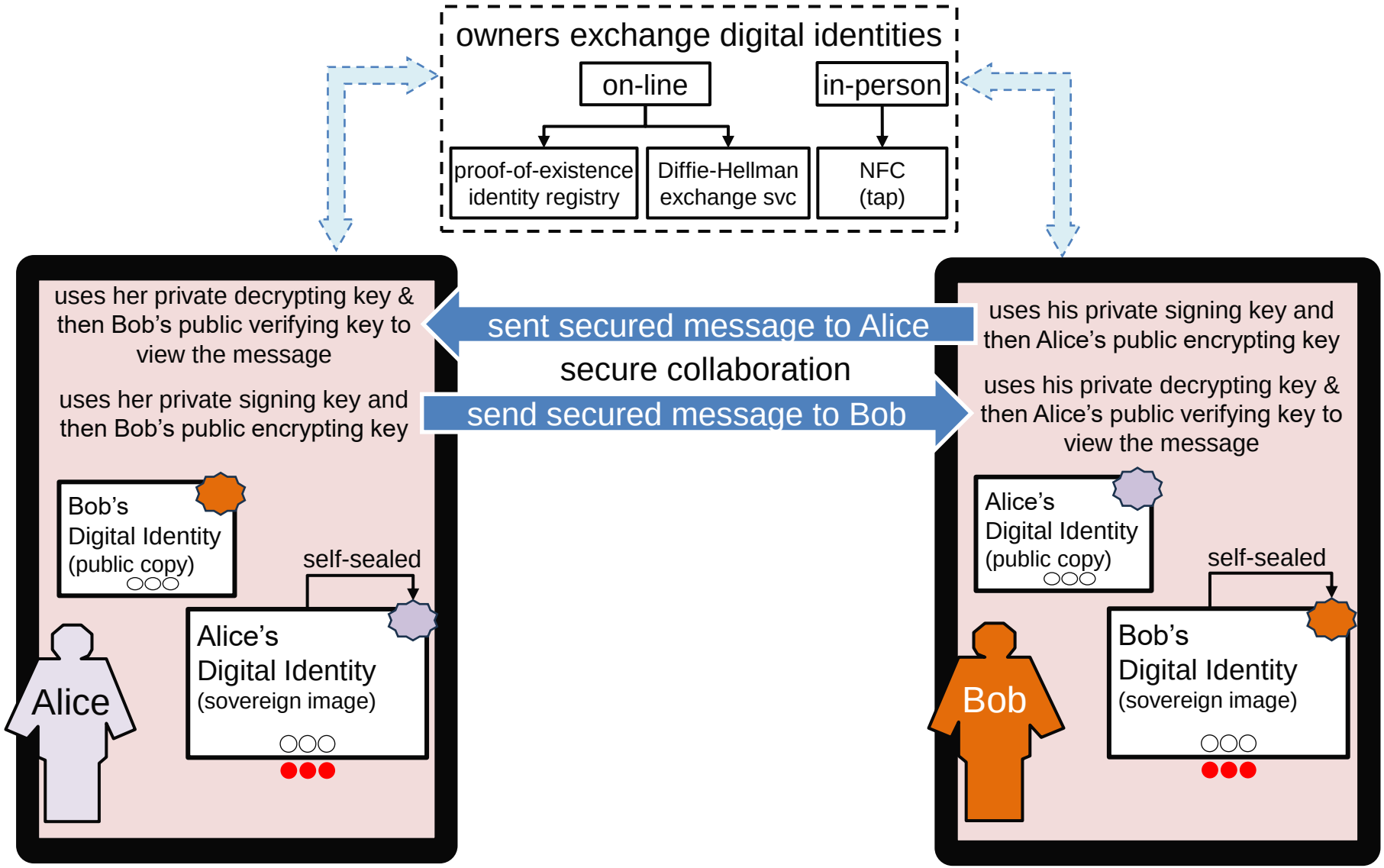
Virtual Identity Layer

(interoperability view)

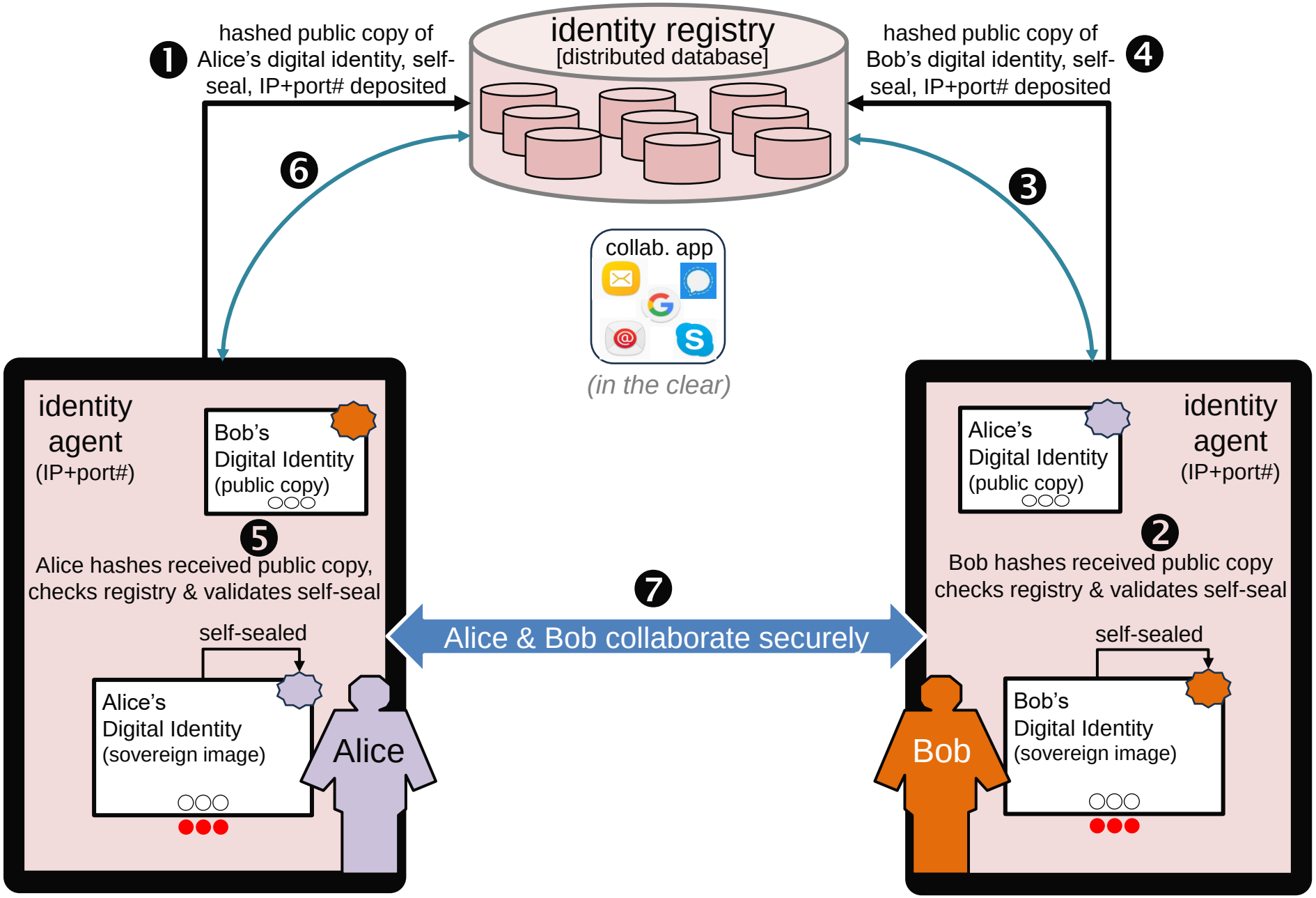


Secure Collaboration: Messages Signed & Encrypted

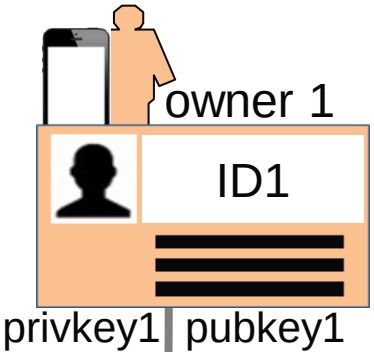
[public copies of digital identities exchanged]

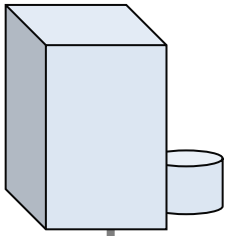


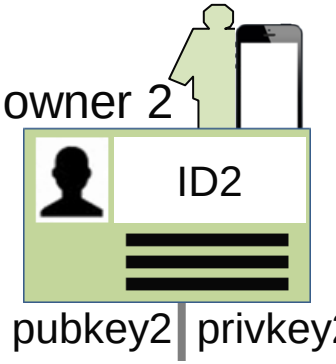
Proof-of-Existence Identity Registry



Digital Identity Exchange Service
(adapted Diffie-Hellman)







privkey1 | pubkey1

OTP1

pubkey2 | privkey2

OTP2

--- transfer OTP1 over alt. channel ----------> OTP1

OTP2 <---------- transfer OTP2 over alt. channel ---

use hash(OTP1)^x to store owner 1's public key →

← use hash(OTP2)^x to store owner 2's public key

use hash(OTP2)^x to get owner 2's public key (pubkey2) ←

use hash(OTP1)^x to get owner 1's public key (pubkey1) →

use Diffie-Hellman
DH (privkey1, pubkey2)
to calc. symmetric key (SK)

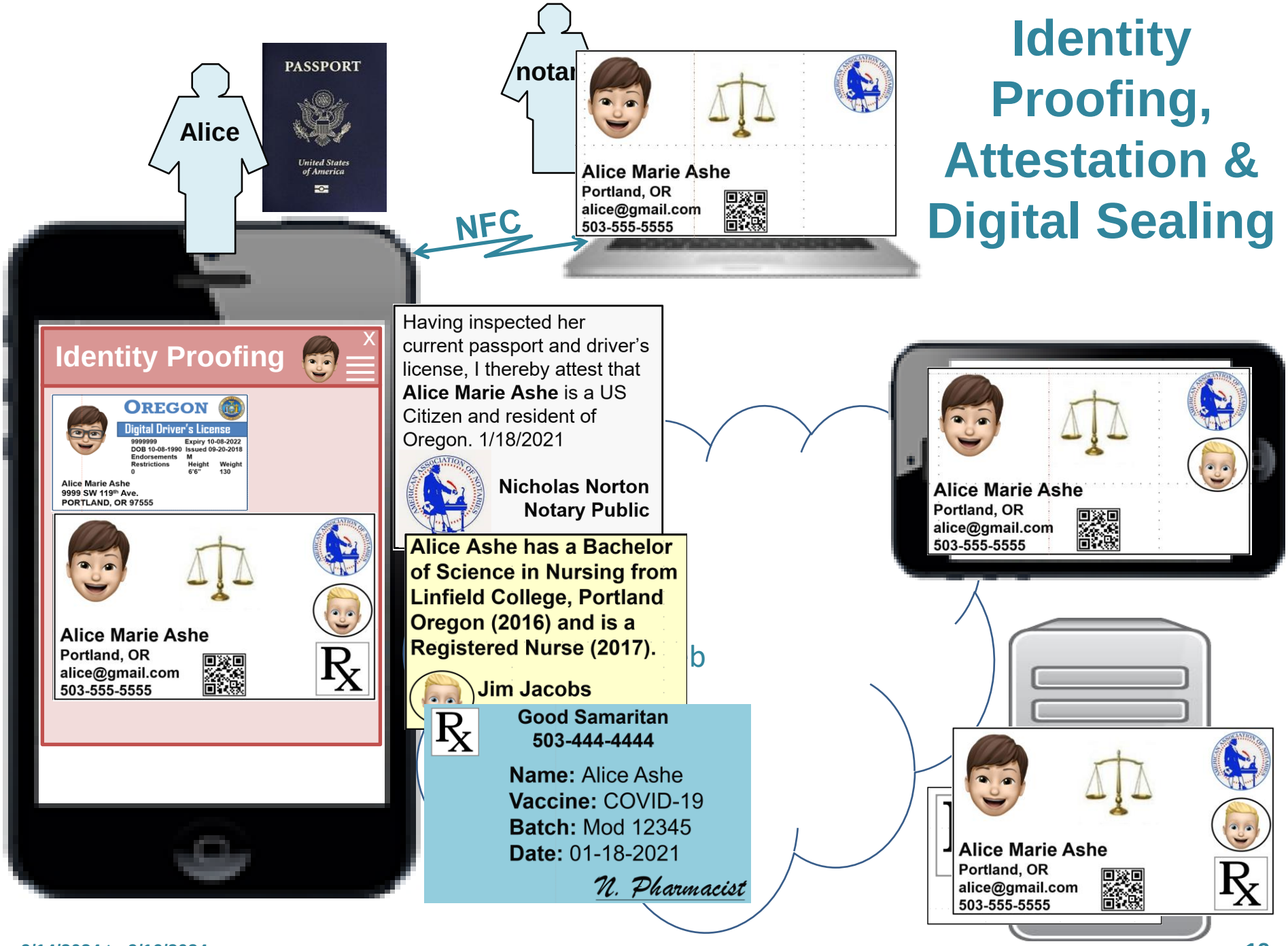
use Diffie-Hellman
DH (privkey2, pubkey1)
to calc. symmetric key (SK)

use SK to encrypt and send owner 1's digital identity to owner 2 →

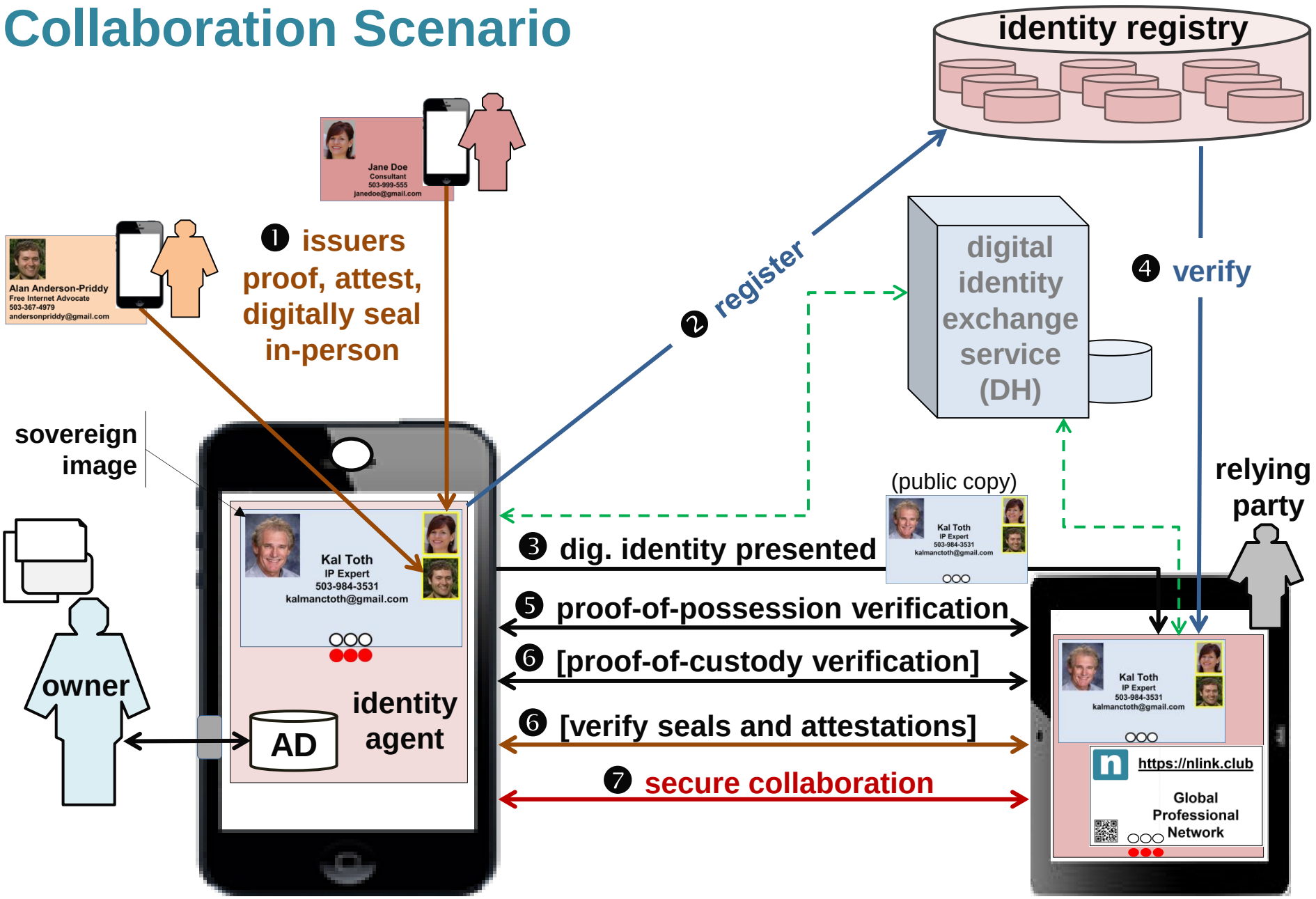
use SK to encrypt and send owner 2's digital identity to owner 2 ←

^{x}. *option: instead of OTPs, public copies of owners' digital identities are hashed and transferred*

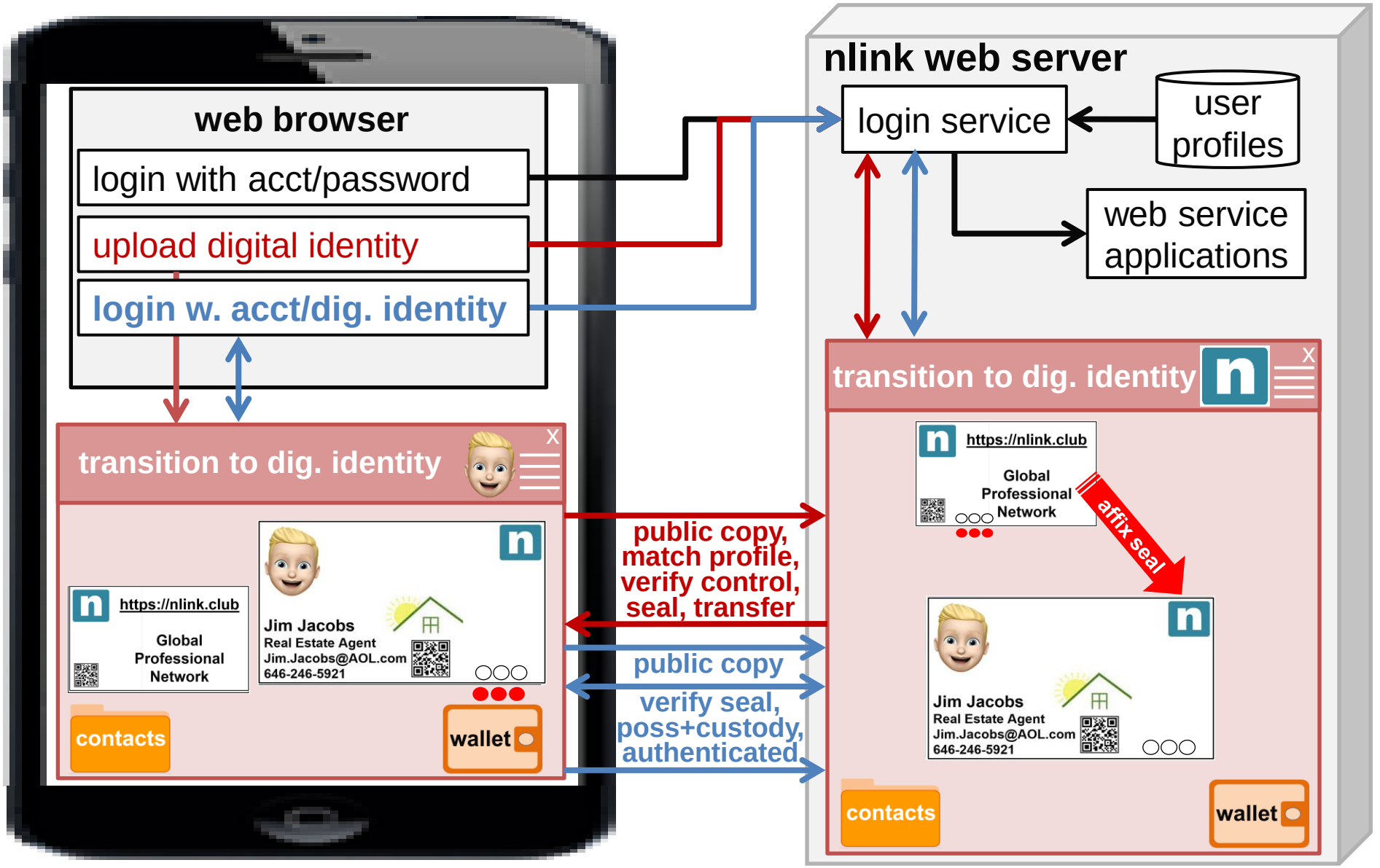
Identity Proofing, Attestation & Digital Sealing



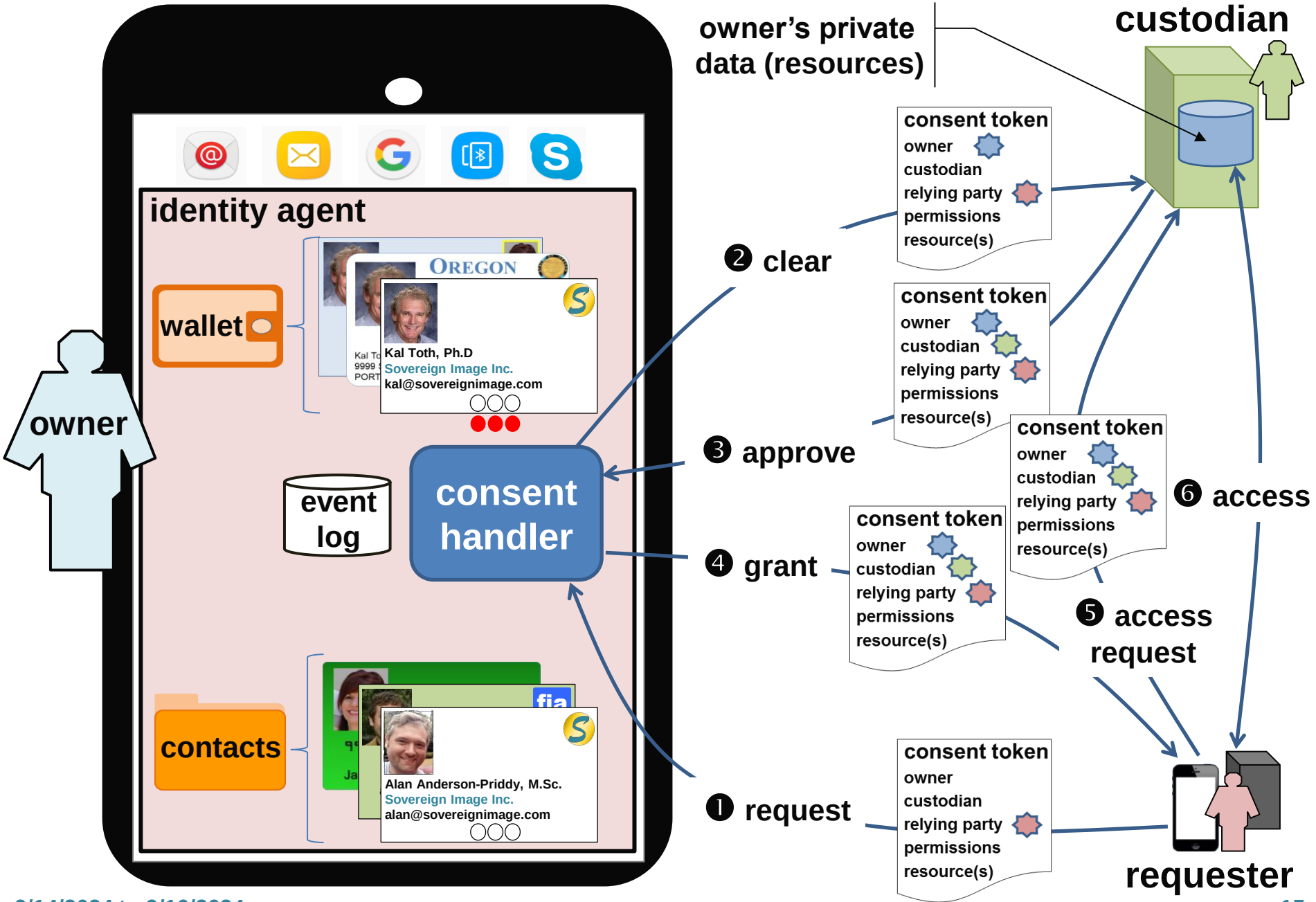
Collaboration Scenario



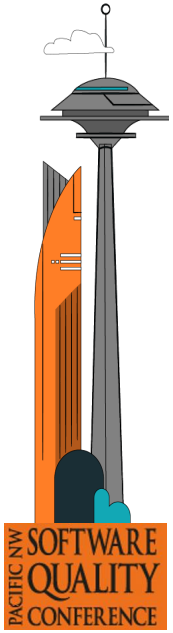
Transitioning from Passwords to Digital Identities



Delegating Consent to Access Private Data



Identity and Authentication Assurance Levels



Adapted National Institute of Science and Technology (NIST) “Identity Assurance and Authentication Assurance” model [14].

Level 0

no authentication and identity assurances

Level 1

Proof-of-existence registry validating digital identities: moderate authentication assurance

Self-attested (self-sealed): weak identity assurance (no identity-proofing)

Level 2

Online Diffie-Hellman digital identity exchange: strong authentication assurance

Identity-proofing using electronic copies of identifying documents: moderate identity assurance

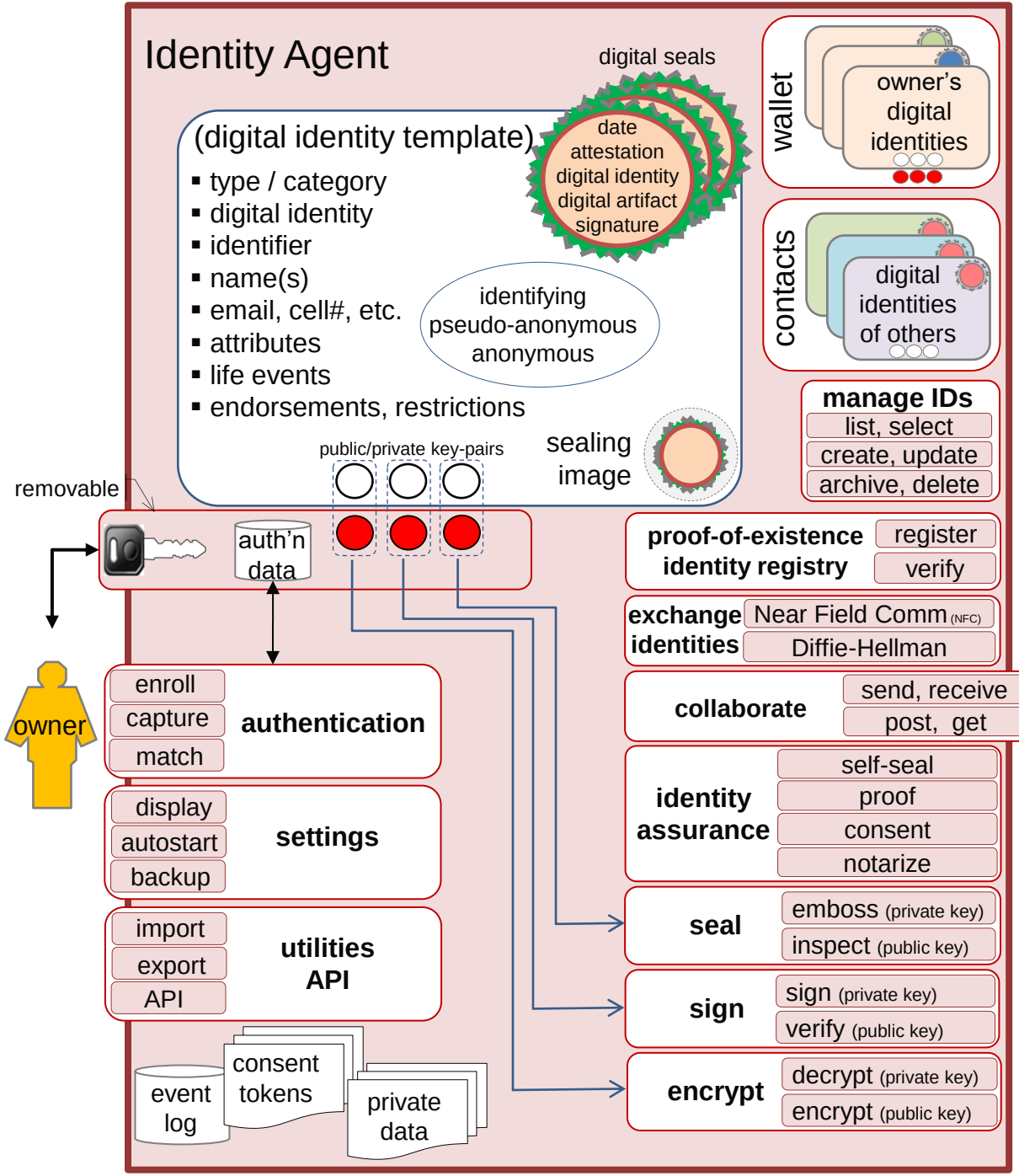
Level 3

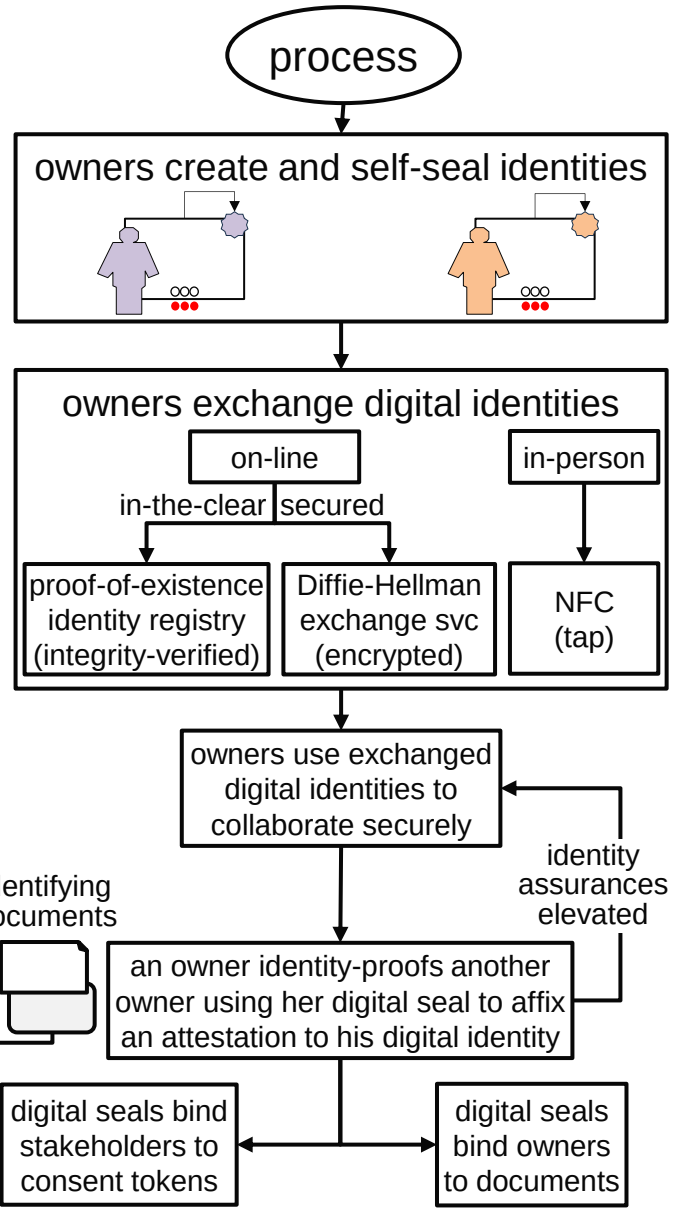
In-person digital identity exchange using NFC: superior authentication assurance

Identity-proofing using physical copies of original issued documents: superior identity assurance

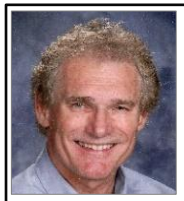
Reference Model

Agent-Based Digital Identity Architecture



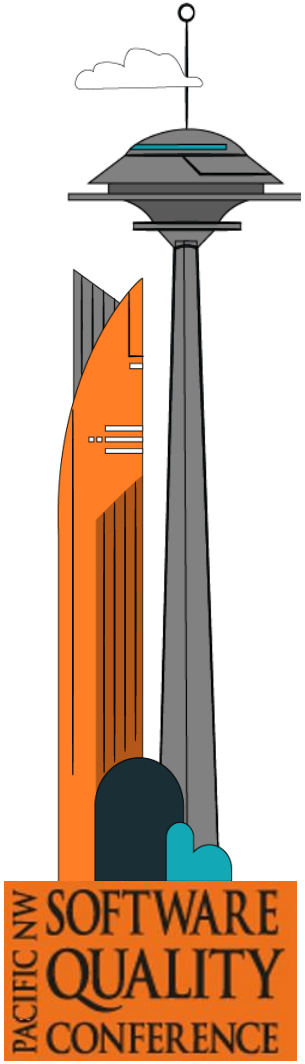


Thank you for your valuable time, questions and comments.



Kal Toth

Kalman C. Toth, Ph.D, P.Eng.
kalmanctoth@gmail.com
https://www.sovereignimage.com
https://www.linkedin.com/in/kaltoth/



Abstract, Bio, Paper, Presentation Slides

PNSQC 2024 “at-a-glance” and “technical papers”

https://www.pnsqc.org/kal_toth_2024.php

http://www.sovereignimage.com/PNSQC2024/

Backup Slides

Digital Identities: Virtualized Physical Identities

Mimic identities / credentials in your wallet

- Intuitive, ease-of-use and facilitate technology adoption

❑ Common Template

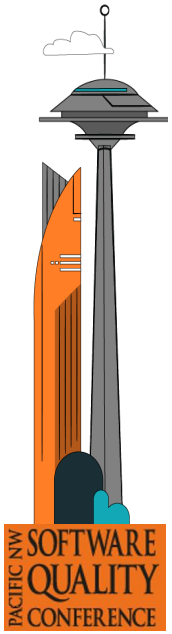
- Potentially customizable by identity agents of owners & service providers
- Categories: identifying, pseudo-anonymous, anonymous (incognito)
- Types: DMV, passport, banking, credit, health, business, personal, etc.
- Identifier, name (legal, informal, pseudonym)
- Issue date, expiry date, endorsements, restrictions
- Identifying attributes (if any) including photo(s)
- Endorsements, restrictions, limitations
- Private/public key-pairs (3)
- Sealing image

❑ Private/public Key-Pairs (3)

- signing/verifying; decrypting/encrypting, embossing/inspecting
- sealing image: virtualize notarizing seals

❑ "Sovereign Image" Versus "Public Copy"

- "Sovereign Image": held by owner hold both the private and public keys
- "Public copies": held by non-owners hold only the public keys



Digital Seals, Attestation, Self-Sealing

Digital Seals

- Analogous to seals affixed by notaries to physical documents.
- Identity agent owners use digital seals to affix attestations to artifacts
- e.g. to digital identities[1], consent tokens, and documents.

❑ Using digital seals to affix an attestation to a digital artifact

- Owner specifies a pertinent attestation.
- Owner selects one of her digital identities.
- Owner's identity agent applies embossing key to create the digital seal.

❑ Creating the digital seal

- Digest: issue date + attestation + pub copy of digital identity + artifact identifier
- Digital seal signature: encrypted digest using embossing key.
- Digital seal: rendered using sealing image and identifying fields.

❑ Digital seal verification

- Inspecting key of digital identity identified in digital seal verifies the signature.

[1.] **Self-sealing:** The embossing key of a digital identity (a sovereign image) is applied to digitally seal the digital identity of an owner (a.k.a. self-attesting)

Impersonation Prevention
(Possession, Custody, Self-Sealing)

Impersonation Risk

- Hackers may present public copies of digital identities fraudulently
- Proof-of-possession, proof-of-custody, self-seal verification eliminate this risk

❑ Proof-of-Possession Challenge

- An identity agent receiving a public copy of a digital identity uses encryption key to encrypt a random value returning the result to sending identity agent.
- This agent decrypts the result and returns it to the receiving agent – if the encrypted value does not match the random value the session is closed.

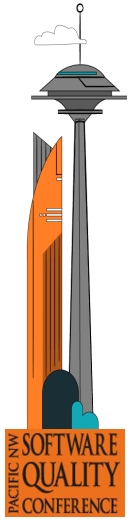
❑ Proof-of-Custody Challenge

- If proof-of-possession is success fully validated, the receiving identity agent can send a demand to the sending agent to authenticate the sending owner.
- Positive confirmation indicates the owner controls the device (is present).

❑ Self-Seal Verification

- The embossing key of a digital identity (sovereign image) is applied to digitally seal the digital identity of an owner (a.k.a. self-attested).
- The inspecting key can be used to verify the digital seal signature.

Elevating Identity Assurances
Identity Proofing and Digital Seals



Identity-proofing a subject (another identity agent owner):
- 3rd party examination of identifying documents in-person or online.

Attestation (e.g. “proofed”):
- Declaring subject successfully identity-proofed.

Digital Sealing an Attestation:
- Using a digital seal to affix an attestation to a digital identity of the subject.

Identity assurances elevated when:
- Identity-proofing is in-person rather than online
- Using notarized copies of identifying documents rather than digital copies
- Using original identifying documents.

Transitioning from using Passwords to using Digital Identities

Pre-conditions:

- **Jim** has used his entity agent to create his digital business card (dig. identity)
- **nlink** has an installed identity agent and a corporate digital identity

Jim logs in with password and uploads his digital Identity

- **Jim** successfully logs in using his **nlink** account / password
- Public copy of **Jim's** digital business card is uploaded to **nlink**

Control verified; profile matched; identity digitally sealed

- **nlink's** identity agent verifies **Jim** controls his dig. identity (possession+custody)
- **nlink** verifies **Jim's** digital business card conforms with his online user profile
- **nlink's** identity engine uses the corporate digital identity to digitally seal **Jim's** digital business card and return it to **Jim's** identity agent

Jim can use his digital business card to authenticate to the **nlink**